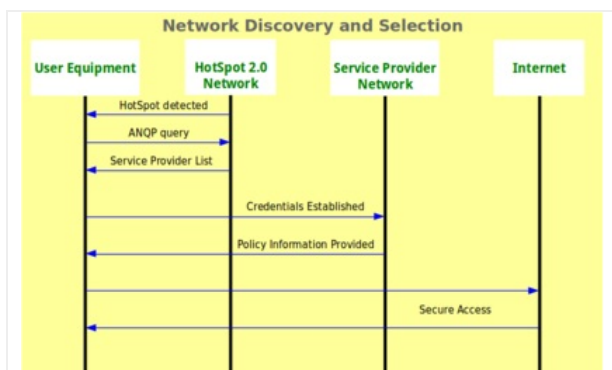
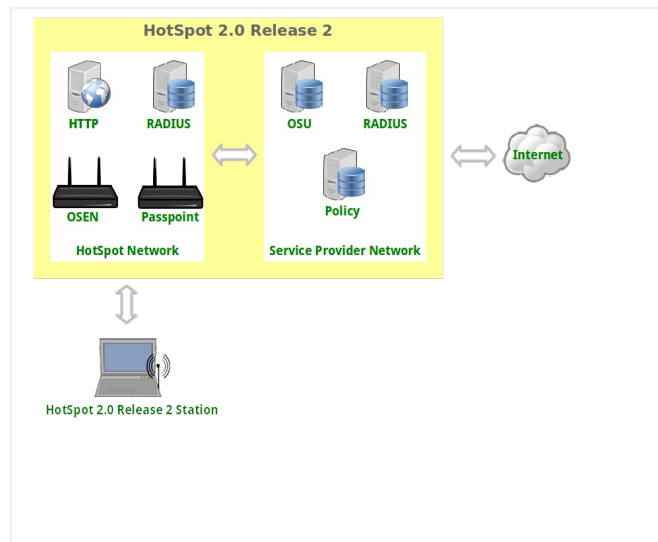


LANforge WiFi testing HotSpot 2.0 Release 2

Goal: Setup HotSpot 2.0 Release 2 Example

Requires LANforge 5.3.2 or later on Fedora 20 or later.

- Run LANforge install script to begin setup of HotSpot 2.0 R2 related servers and certificates.
- Configure the **OSU Server-only** authenticated layer-2 **Encryption Network (OSEN)** AP and Passpoint AP.
- Initiate **Online Sign-Up (OSU)** procedure, select a provider and obtain an IP address from the Passpoint AP.
- Send traffic through the Service Provider Network.



For more information see:

WiFi Alliance Passpoint Release 2 Deployment Guidelines

<https://www.wi-fi.org/file/passpoint-release-2-deployment-guidelines>

1. Run LANforge installation script to begin hostapd RADIUS, certificates and HotSpot 2.0 setup:

```
cd /home/lanforge
./lf_install.pl --lfver 5.3.2 --do_radius --do_hs20
```

2. Make two copies of the `ca.pem` certificate to different directories:

```
cp /home/lanforge/hs20/ca/ca.pem /home/lanforge/ota-ca.pem
cp /home/lanforge/hs20/ca/ca.pem /home/lanforge/wifi/osu_wlan2/osu-ca.pem
```

ota-ca.pem is used by the client for Over-The-Air authentication to the OSEN AP

osu-ca.pem is used by the client for the Online-Sign-Up server authentication before connecting to the Passpoint AP

This is an all-in-one example on a single LANforge system, but if the authentication servers were setup on different systems, the proper certificates would need to be copied instead.

3. Create `devinfo.xml` and `devdetail.xml` files in `/home/lanforge/wifi/osu_wlan2`

A. /home/lanforge/wifi/osu_wlan2/devinfo.xml

```
<DevInfo xmlns="urn:oma:mo:oma-dm-devinfo:1.0">
  <DevId>urn:Example:HS20-station:123456</DevId>
  <Man>Manufacturer</Man>
  <Mod>HS20-station</Mod>
  <DmV>1.2</DmV>
  <Lang>en</Lang>
</DevInfo>
```

B. /home/lanforge/wifi/osu_wlan2/devdetail.xml

```
<DevDetail xmlns="urn:oma:mo:oma-dm-devdetail:1.0">
  <Ext>
    <org.wi-fi>
      <Wi-Fi>
        <EAPMethodList>
          <EAPMethod1>
            <EAPType>13</EAPType>
          </EAPMethod1>
          <EAPMethod2>
            <EAPType>21</EAPType>
            <InnerMethod>MS-CHAP-V2</InnerMethod>
          </EAPMethod2>
          <EAPMethod3>
            <EAPType>18</EAPType>
          </EAPMethod3>
          <EAPMethod4>
            <EAPType>23</EAPType>
          </EAPMethod4>
          <EAPMethod5>
            <EAPType>50</EAPType>
          </EAPMethod5>
        </EAPMethodList>
        <ManufacturingCertificate>>false</ManufacturingCertificate>
        <Wi-FiMACAddress>020102030405</Wi-FiMACAddress>
        <IMSI>310026000000000</IMSI>
        <IMEI_MEID>imei:490123456789012</IMEI_MEID>
        <ClientTriggerRedirectURI>http://localhost:12345</ClientTriggerRedirectURI>
        <Ops>
          <launchBrowserToURI></launchBrowserToURI>
          <negotiateClientCertTLS></negotiateClientCertTLS>
          <getCertificate></getCertificate>
        </Ops>
      </Wi-Fi>
    </org.wi-fi>
  </Ext>
  <URI>
    <MaxDepth>0</MaxDepth>
    <MaxTotLen>0</MaxTotLen>
    <MaxSegLen>0</MaxSegLen>
  </URI>
  <DevType>MobilePhone</DevType>
  <OEM>Manufacturer</OEM>
  <FwV>1.0</FwV>
  <SwV>1.0</SwV>
  <HwV>1.0</HwV>
  <LrgObj>false</LrgObj>
</DevDetail>
```

4. Create two MAC-VLANs for two hostapd RADIUS server instances.

A. Go to the Port Manager tab, select eth1, select Create, select MAC-VLAN, quantity 2 then Apply.

B. Double-click each new MAC-VLAN interface in the Port-Mgr tab to modify. Select the RADIUS checkbox which will allow a hostapd based RADIUS server on the interfaces using the config files: /home/lanforge/wi fi/hostapd_eth1#0.conf and /home/lanforge/wi fi/hostapd_eth1#1.conf

Because this is an all-in-one example, the hostapd RADIUS servers will be referenced to localhost and each MAC-VLAN interface will not need an IP address assigned. If the hostapd RADIUS servers were on different systems or networks, the appropriate IP address would be assigned here.

C. Create config file:

`/home/lanforge/wifi/hostapd_eth1#0.conf` for the hostapd RADIUS server on eth1#0.

NOTE: The `eap_user_file`, `eap_sim_db` and `radius_server_auth_port` are unique for each RADIUS server.

```
interface=eth1#0
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
dump_file=/home/lanforge/wifi/hostapd_eth1#0.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/home/lanforge/hs20/AS/hostapd-osen.eap_user
server_id=ct523-3n-f20
eap_sim_db=unix:/tmp/hlr_auc_gw.sock
radius_server_auth_port=1820
radius_server_clients=/home/lanforge/hs20/AS/hostapd.radius_clients

ca_cert=/home/lanforge/hs20/ca/ca.pem
server_cert=/home/lanforge/hs20/ca/server.pem
private_key=/home/lanforge/hs20/ca/server.key
private_key_passwd=lanforge

ocsp_stapling_response=/home/lanforge/hs20/ca/ocsp-server-cache.der
```

D. Create config file:

`/home/lanforge/wifi/hostapd_eth1#1.conf` for the hostapd RADIUS server on eth1#1.

NOTE: The `eap_user_file`, `eap_sim_db` and `radius_server_auth_port` are unique for each RADIUS server.

```
interface=eth1#1
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
dump_file=/home/lanforge/wifi/hostapd_eth1#1.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=sqlite:/home/lanforge/hs20/AS/DB/eap_user.db
server_id=ct523-3n-f20
eap_sim_db=unix:/tmp/hlr_auc_gw.sock db=/home/lanforge/hs20/AS/DB/eap_sim.db
radius_server_auth_port=1821
radius_server_clients=/home/lanforge/hs20/AS/hostapd.radius_clients

ca_cert=/home/lanforge/hs20/ca/ca.pem
server_cert=/home/lanforge/hs20/ca/server.pem
private_key=/home/lanforge/hs20/ca/server.key
private_key_passwd=lanforge

ocsp_stapling_response=/home/lanforge/hs20/ca/ocsp-server-cache.der
```

E. Start the `hlr_auc_gw` tool:

```
cd /home/lanforge
. lanforge.profile
hlr_auc_gw -m /etc/hlr_auc_gw.milenage_db > /tmp/hlr_auc_gw.log &
```

NOTE: If the `hlr_auc_gw` does not start, you may have to remove the file `/tmp/hlr_auc_gw.sock` first.

- F. Reset the MAC-VLAN interfaces on the Port Mgr tab so that the new hostapd RADIUS servers are started. Check that they are running with the command:

```
ps auxwww |grep hostapd_eth
```

If they are not running, check the log files for problems:

```
cat /home/lanforge/wifi/hostapd_log_eth1#0.txt
cat /home/lanforge/wifi/hostapd_log_eth1#1.txt
```

5. Create two VAPs for the HotSpot 2.0 Release 2 Network.
- Go to the Port Mgr tab and create one VAP on wiphy0 and one VAP on wiphy1.
 - Modify the first VAP on wiphy0 to be the **OSEN** AP. Configure IP Address and SSID.

vap1 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: LINK-UP GRO NONE
 Driver Info: Port Type: WIFI-AP Parent: wiphy0

Port Configurables

Standard Configuration | Advanced Configuration | Misc Configuration | Custom WiFi

Enable

- Set IF Down
- Set MAC
- Set TX Q Len
- Set MTU
- Set Offload
- Set PROMISC

Services

- HTTP
- FTP

Low Level

- PROMISC
- TSO Enabled
- UFO Enabled
- GSO Enabled
- LRO Enabled
- GRO Enabled

General Interface Settings

- Down
- DHCP-IPv6
- DHCP-IPv4
- Aux-Mgt
- DHCP Release
- DHCP Vendor ID: None
- DHCP Client ID: None
- DNS Servers: BLANK
- IP Address: 10.88.1.1
- IP Mask: 255.255.255.0
- Gateway IP: 0.0.0.0
- Alias:
- MAC Addr: 00:0e:8e:5d:5a:71
- Rpt Timer: faster (1 s)
- Peer IP: NA
- Global IPv6: AUTO
- Link IPv6: AUTO
- IPv6 GW: AUTO
- MTU: 1500
- TX Q Len: 1000
- WiFi Bridge: NONE

WiFi Settings

- SSID: ABCD-1234
- Key/Phrase:
- Freq/Channel: 5180/36
- DTIM-Period: 2
- Beacon: 240
- AP: DEFAULT
- Mode: 802.11abgn
- Rate: OS Default
- Max-STA: 2007
- WPA
- WPA2
- OSEN
- WEP
- Disable HT40
- Disable HT80
- Disable SGI
- Verbose Debug

Print | View Details | Logs | Probe | Display Scan | Sync | Apply | OK | Cancel

- C. Select the **Advanced Configuration** tab in the Port-Modify window to configure 802.1x and RADIUS server information.

The screenshot shows the 'vap1 (ct523-3n-f20) Configure Settings' window. The 'Advanced Configuration' tab is selected. The 'Advanced WiFi Settings' section is visible, containing various configuration options. The 'RADIUS IP' is set to '127.0.0.1', 'RADIUS Port' is '1820', and 'RADIUS Secret' is 'lanforge'. The 'Advanced/802.1x' checkbox is checked, while 'Enable 802.11u' is unchecked. Other options like 'Ignore Probes', 'Ignore Auth-Assoc', and 'Ignore Assoc' are set to 'zero (0%)'. The 'Use 80211d', 'Use 80211h', and 'Short-Preamble' checkboxes are also unchecked.

- D. Select the **Custom WiFi** tab to add the following lines for HotSpot 2.0 Release 2.

```
ocsp_stapling_response=/home/lanforge/hs20/ca/ocsp-server-cache.der
```

The screenshot shows the 'vap1 (ct523-3n-f20) Configure Settings' window with the 'Custom WiFi' tab selected. The 'Custom WiFi' section is visible, containing a text area for 'User-Specified supplicant/hostapd configuration text:'. The text area contains the following line: 'ocsp_stapling_response=/home/lanforge/hs20/ca/ocsp-server-cache.der'. The 'Apply' button is highlighted.

E. Modify the second VAP on wiphy1 to be the **Passpoint** AP. Configure IP Address and SSID.

vap2 (ct523-3n-f20) Configure Settings

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy1

Port Configurables

Standard Configuration | **Advanced Configuration** | Misc Configuration | Custom WiFi

Enable

- Set IF Down
- Set MAC
- Set TX Q Len
- Set MTU
- Set Offload
- Set PROMISC

Services

- HTTP
- FTP

Low Level

- PROMISC
- TSO Enabled
- UFO Enabled
- GSO Enabled
- LRO Enabled
- GRO Enabled

General Interface Settings

- Down Aux-Mgt
- DHCP-IPv6 DHCP Release DHCP Vendor ID: None
- DHCP-IPv4 **Secondary-IPs** DHCP Client ID: None
- DNS Servers: BLANK Peer IP: NA
- IP Address: 10.1.1.1 Global IPv6: AUTO
- IP Mask: 255.255.255.0 Link IPv6: AUTO
- Gateway IP: 0.0.0.0 IPv6 GW: AUTO
- Alias: MTU: 1500
- MAC Addr: 00:0e:8e:23:17:48 TX Q Len: 1000
- Rpt Timer: medium (8 s) WiFi Bridge: NONE

WiFi Settings

- SSID: ABCD-5678 AP: DEFAULT
- Key/Phrase: Mode: 802.11abgn
- Freq/Channel: 5180/36 Rate: OS Default
- DTIM-Period: 2 Max-STA: 2007
- Beacon: 240
- WPA WPA2 OSEN WEP Disable HT40 Disable HT80 Disable SGI
- Verbose Debug

Print View Details Logs Probe Display Scan Sync Apply OK Cancel

F. Select the **Advanced Configuration** tab in the Port-Modify window to configure 802.1x, 802.1u, HotSpot 2.0, RADIUS server and other information.

vap2 (ct523-3n-f20) Configure Settings

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy1

Port Configurables

Standard Configuration | **Advanced Configuration** | Misc Configuration | Custom WiFi

Advanced WiFi Settings

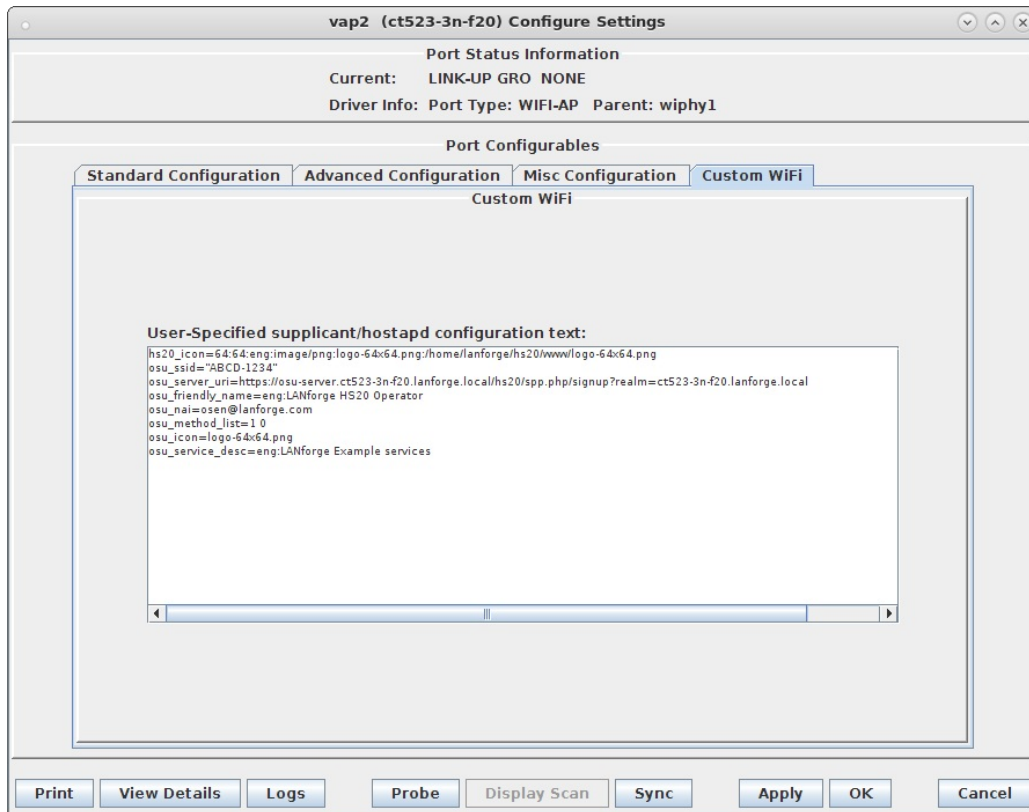
Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

- Ignore Probes: zero (0%) HESSID: 00:00:00:00:00:00
- Ignore Auth-Assoc: zero (0%) Realm: 0.ct523-3n-f20.lanforge.local,12[5:6],21[2:4][5:7]
- Ignore Assoc: zero (0%) IMSI:
- Ignore Re-Assoc: zero (0%) Milenage:
- Corrupt GTK: zero (0%) Domain: ct523-3n-f20.lanforge.local
- HS20 Capabilities Consortium:
- HS20 Oper Class RADIUS IP: 127.0.0.1
- HS20 WAN Metrics RADIUS Port: 1821
- IEEE80211w: Disabled (0) RADIUS Secret: lanforge
- Venue Group: Unspecified (0) Venue Type: Unspecified (0)
- Network Type: Private (0) Address Types: Not Available (0)
- Network Auth: 3GPP Cell Net:
- Use 80211d Use 80211h Short-Preamble
- Advanced/802.1x HotSpot 2.0 Disable DGAF
- Enable 802.11u 802.11u Internet 802.11u ASRA 802.11u ESR 802.11u UESA

Print View Details Logs Probe Display Scan Sync Apply OK Cancel

G. Select the **Custom WiFi** tab to add the following lines for HotSpot 2.0 Release 2.

```
hs20_icon=64:64:eng:image/png:logo-64x64.png:/home/lanforge/hs20/www/logo-64x64.png
osu_ssid="ABCD-1234"
osu_server_uri=https://osu-server.ct523-3n-f20.lanforge.local/hs20/spp.php/signup?realm=ct523-3n-f20.lanforge.local
osu_friendly_name=eng:LANforge HS20 Operator
osu_nai=osen@lanforge.com
osu_method_list=1 0
osu_icon=logo-64x64.png
osu_service_desc=eng:LANforge Example services
```



H. Modify wiphy0 and wiphy1 to be on the same channel and select OK.

wiphy0 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: LINK-DOWN NONE
 Driver Info: Port Type: WIFI-Radio Driver: ath9k() Bus:

Port Configurables

Enable

- Set IF Down
- Set MAC
- Set TX Q Len
- Set MTU
- Set Offload
- Set PROMISC

General Interface Settings

Down Aux-Mgt

DHCP-IPv6 DHCP Release DHCP Vendor ID: None

DHCP-IPv4 **Secondary-IPs** DHCP Client ID: None

DNS Servers: BLANK Peer IP: NA

IP Address: 0.0.0.0 Global IPv6: AUTO

IP Mask: 0.0.0.0 Link IPv6: AUTO

Gateway IP: 0.0.0.0 IPv6 GW: AUTO

Alias: MTU: 1500

MAC Addr: 00:0e:8e:43:3a:71 TX Q Len: 0

Rpt Timer: medium (8 s) WiFi Bridge: NONE

WiFi Settings
 Max-VIFs: 2048 Max-Stations: 2048 Max-APs: 8 Supports: 802.11abgn

Country: United States (840)

Channel/Freq: 36 (5180 Mhz)

Antenna: All Tx-Power: DEFAULT

RTS: DEFAULT Frag: 2346

Verbose Debug

Print View Details Logs Probe Sync Apply OK Cancel

wiphy1 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: LINK-DOWN NONE
 Driver Info: Port Type: WIFI-Radio Driver: ath9k() Bus:

Port Configurables

Enable

- Set IF Down
- Set MAC
- Set TX Q Len
- Set MTU
- Set Offload
- Set PROMISC

General Interface Settings

Down Aux-Mgt

DHCP-IPv6 DHCP Release DHCP Vendor ID: None

DHCP-IPv4 **Secondary-IPs** DHCP Client ID: None

DNS Servers: BLANK Peer IP: NA

IP Address: 0.0.0.0 Global IPv6: AUTO

IP Mask: 0.0.0.0 Link IPv6: AUTO

Gateway IP: 0.0.0.0 IPv6 GW: AUTO

Alias: MTU: 1500

MAC Addr: 00:0e:8e:43:37:48 TX Q Len: 0

Rpt Timer: medium (8 s) WiFi Bridge: NONE

WiFi Settings
 Max-VIFs: 2048 Max-Stations: 2048 Max-APs: 8 Supports: 802.11abgn

Country: United States (840)

Channel/Freq: 36 (5180 Mhz)

Antenna: All Tx-Power: DEFAULT

RTS: DEFAULT Frag: 2346

Verbose Debug

Print View Details Logs Probe Sync Apply OK Cancel

I. In Netsmith, setup each VAP with DHCP Service on different IP networks.

J. Check that the VAP hostapd processes are running with the command:

```
ps auxwww |grep hostapd_vap
```

If they are not running, check the log files for problems:

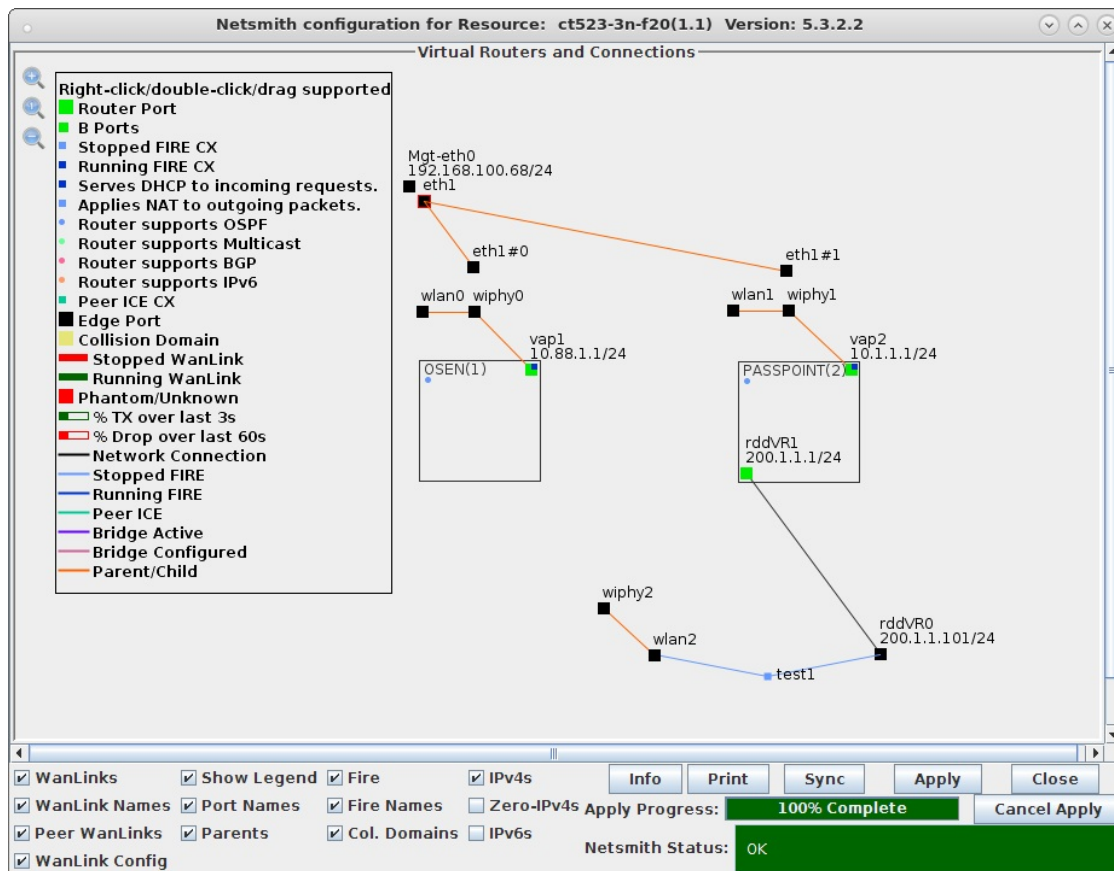
```
tail -f /home/lanforge/wifi/hostapd_log_vap1.txt
tail -f /home/lanforge/wifi/hostapd_log_vap2.txt
```

For more information see [WiFi Testing: Configuring a Virtual AP with Limited Stations](#)

6. Start the **Online Certificate Status Protocol (OCSP)** script which will restart the OCSP Responder and update the cache once per minute. It is only required on the VAP or server side of a HotSpot 2.0 R2 network.

```
cd /home/lanforge
./ocsp.bash > /dev/null 2>&1 &
```

7. In Netsmith, we can label the two Virtual Routers containing each VAP. We also setup a single TCP connection named 'test1' between the client (wlan2) and a virtual interface connected to the Passpoint AP. In this way, we can verify that the client is only allowed to pass traffic once it has met the authentication requirements for the HotSpot and Service Provider Networks.



For more information see

, [Virtual Router with NAT Cookbook](#) , [Virtual Router with DHCP Cookbook](#)

8. Setup wlan2 as the HotSpot 2.0 R2 client.

- A. Modify wlan2 on the Port Mgr tab and set the SSID to the OSEN AP's SSID 'ABCD-1234' in this example and set the authentication to **OSEN**.

wlan2 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: DOWN LINK-DOWN GRO NONE
 Driver Info: Port Type: WIFI-STA Parent: wiphy2

Port Configurables

Standard Configuration | Advanced Configuration | Misc Configuration | Custom WiFi

Enable

- Set IF Down
- Set MAC
- Set TX Q Len
- Set MTU
- Set Offload
- Set PROMISC

Services

- HTTP
- FTP
- RADIUS

Low Level

- PROMISC
- TSO Enabled
- UFO Enabled
- GSO Enabled
- LRO Enabled
- GRO Enabled

General Interface Settings

Down Aux-Mgt

DHCP-IPv6 DHCP Release DHCP Vendor ID: None

DHCP-IPv4 DHCP Client ID: None

DNS Servers: BLANK Peer IP: NA

IP Address: 0.0.0.0 Global IPv6: AUTO

IP Mask: 0.0.0.0 Link IPv6: AUTO

Gateway IP: 0.0.0.0 IPv6 GW: AUTO

Alias: MTU: 1500

MAC Addr: 00:03:7f:00:00:00 TX Q Len: 1000

Rpt Timer: faster (1 s) WiFi Bridge: NONE

WiFi Settings

SSID: ABCD-1234 AP: DEFAULT

Key/Phrase: Mode: 802.11abgn-AC

Freq/Channel: 5180/36 Rate: OS Default

WPA WPA2 OSEN WEP Disable HT40 Disable SGI

Print View Details Probe Display Scan Sync Apply OK Cancel

- B. In wlan2 Advanced WiFi Settings, select Advanced/802.1x, set Key Management, EAP Identity and CA Cert File.

wlan2 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: DOWN LINK-DOWN GRO NONE
 Driver Info: Port Type: WIFI-STA Parent: wiphy2

Port Configurables

Standard Configuration | Advanced Configuration | Misc Configuration | Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

Key Management: OSEN HESSID: 00:00:00:00:00:00

Pairwise Ciphers: DEFAULT Realm:

Group Ciphers: DEFAULT Client Cert:

WPA PSK: IMSI:

EAP Methods: DEFAULT Milenage:

EAP Identity: osen@lanforge.com Domain:

EAP Anon Identity: Consortium:

EAP Password: Phase-1:

EAP Pin: Phase-2:

Private Key: PK Password:

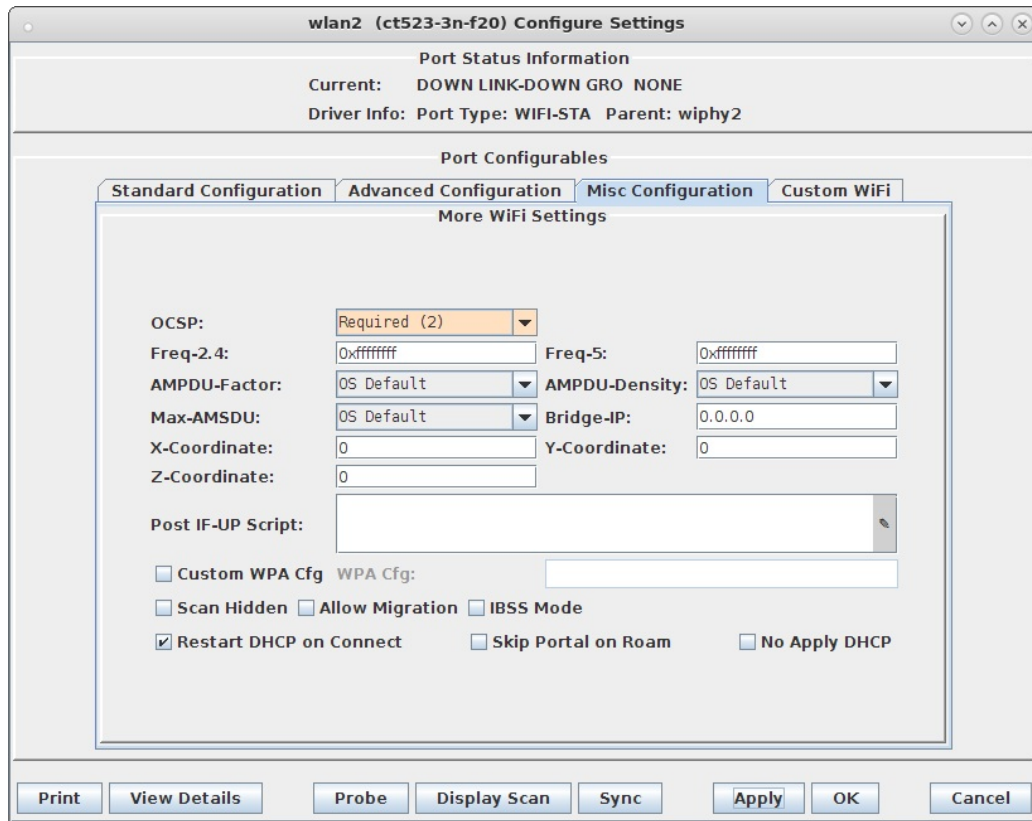
CA Cert File: /home/lanforge/ota-ca.pem PAC File:

Network Auth: Ieee80211w: Disabled (0)

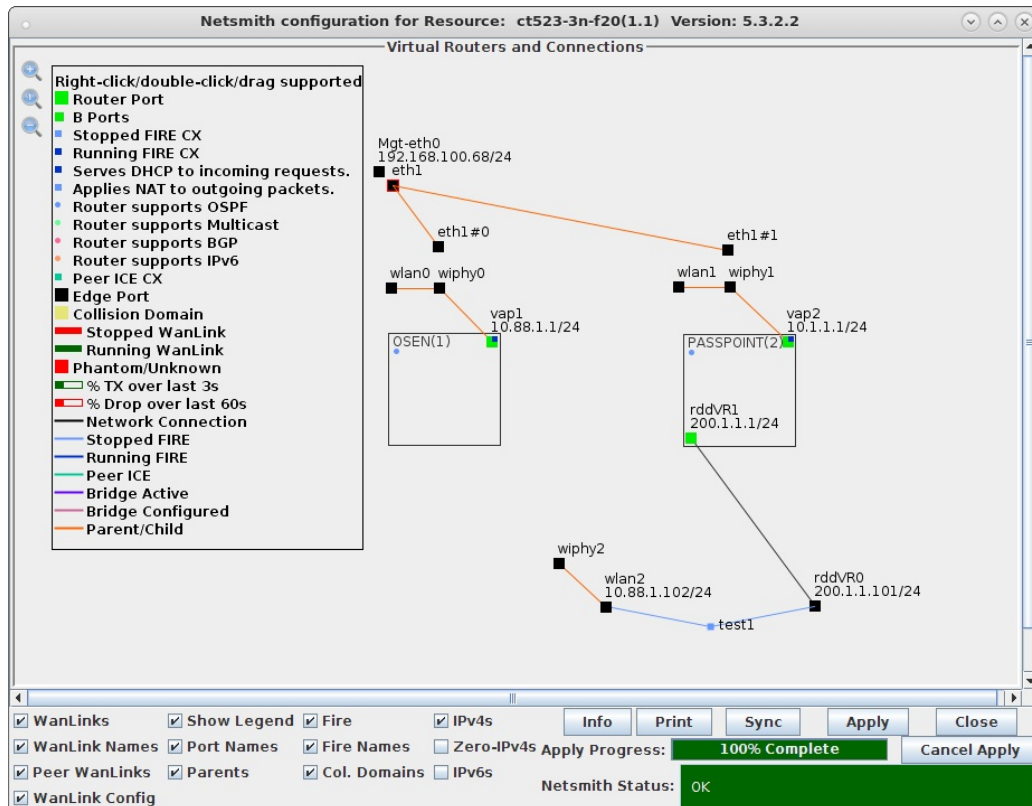
Advanced/802.1x Enable 802.11u HotSpot 2.0 Enable PKC

Print View Details Probe Display Scan Sync Apply OK Cancel

C. In wlan2 Misc Configuration, set OCSP to Required.



D. Admin up wlan2 and it will associate with the OSEN AP and obtain an IP address on the OSEN AP IP network.

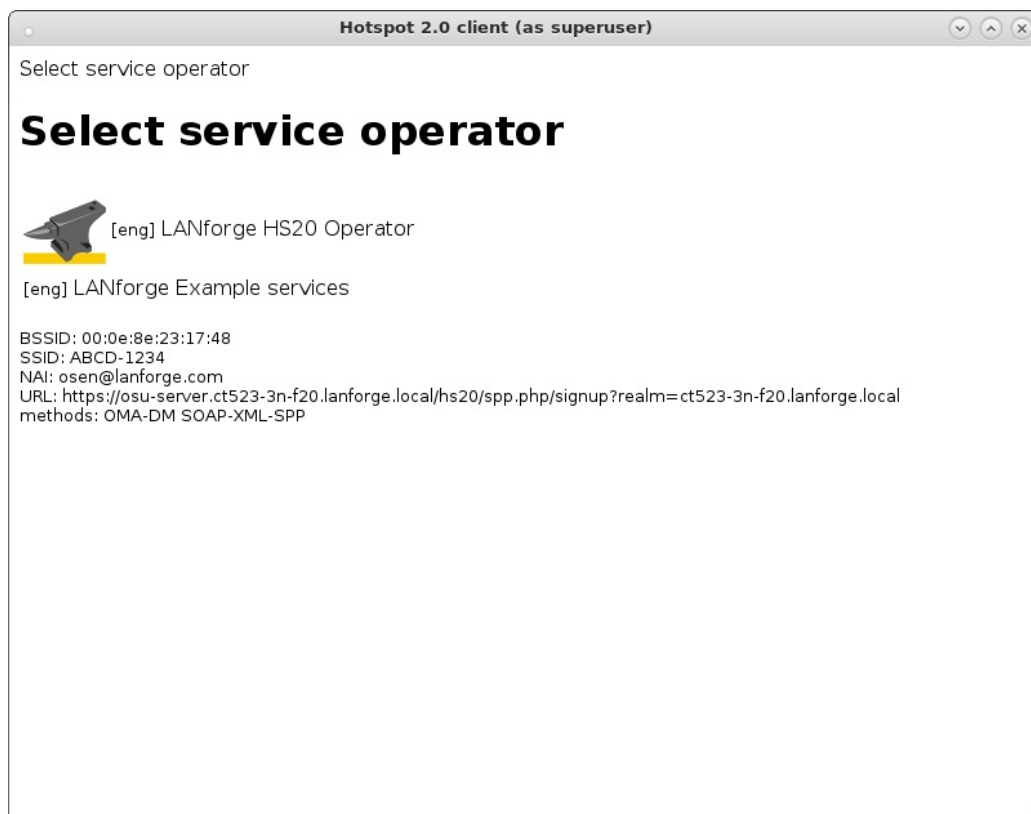


9. Initiate Online Sign-Up

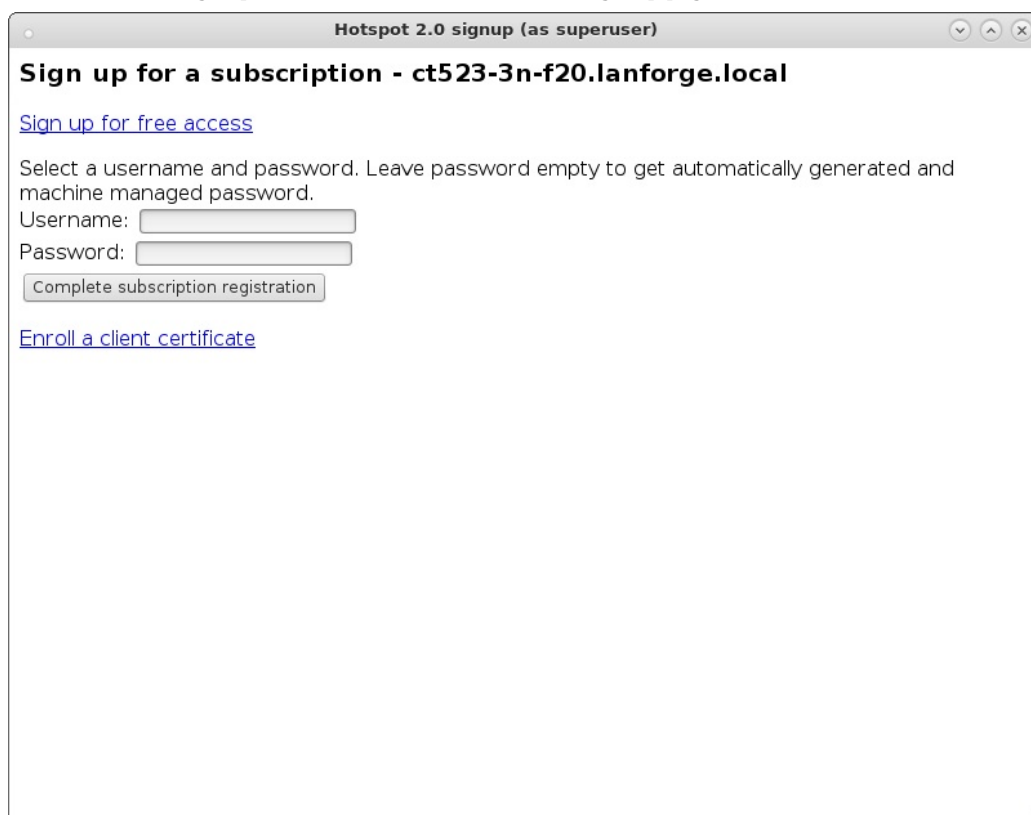
A. In a terminal window type the following:

```
cd /home/lanforge/wifi/osu_wlan2
~lanforge/local/hs20/client/hs20-osu-client -x /home/lanforge/local/hs20/spp/spp.xsd -dd -S wlan2 signup
```

B. Select 'LANforge HS20 Operator' from the Service Provider List.



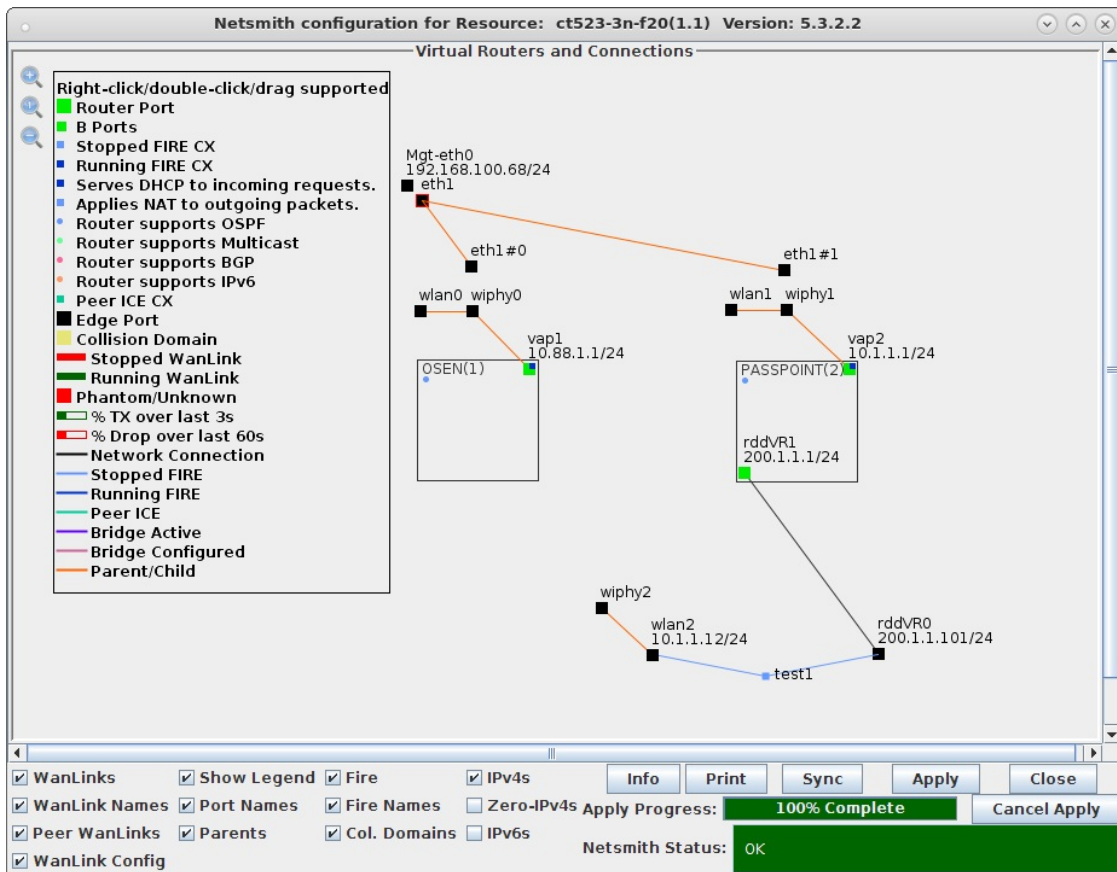
C. Select 'Sign up for free access' from the Online Sign-Up page.



D. Select the Accept button to complete the Online Sign-Up.



10. Client wlan2 will obtain an IP address on the Passpoint AP IP network and TCP connection 'test1' can now pass traffic.



LANforge Manager Version(5.3.2.2)

Control Reporting Tear-Off Info Plugins

Stop All Restart Manager Refresh HELP

File-IO Layer-4 Generic Test Mgr Test Group Resource Mgr Event Log Alerts Port Mgr Messages
 Status Layer-3 L3 Endps VoIP/RTP VoIP/RTP Endps Armageddon WanLinks Attenuators Collision-Domains

Rpt Timer: default (5 s) Go Test Manager all Select All Start Stop Quiesce Clear

View 0 - 200 Display Create Modify Delete

Cross Connects for Selected Test Manager

Name	Type	State	Pkt Rx A	Pkt Rx B	Bps Rx A	Bps Rx B	Rx Drop % A	Rx Drop % B	Drop Pkts A	Drop Pkts B
test1	LF/TCP	Run	201	203	1,539,146	1,541,123	0	0	0	0

Logged in to: localhost:4002 as: Admin

- If wlan2 is reset or reassociates with the OSEN AP, you will have to remove the Service Provider (SP) directory before attempting the Online Sign-Up again.

```
cd /home/lanforge/wifi/osu_wlan2
rm -rf SP
```